BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-202

22 JUNE 2000

Communications and Information

COMPUTER SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil.

OPR: HQ AFCA/GCI (SMSgt Harwell)
Supersedes AFI 33-202, 1 February 1999

Certified by: HQ USAF/SCXX (Lt Col Pricer)
Pages: 37
Distribution: F

This instruction implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and establishes Air Force COMPUSEC requirements for information protection to comply with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*; and Department of Defense Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AIS)*, March 21, 1988. You may use extracts from this Air Force instruction (AFI). Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCI, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5222, and HQ Air Force Communications and Information Center (HQ AFCIC/SYI), 1250 Air Force Pentagon, Washington DC 20330-1250. For a glossary of references and supporting information refer to **Attachment 1** and AFDIR 33-303, *Compendium of Communications and Information Technology*. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

Updates purpose paragraph to include trade name statement. Adds paragraph **2.5.3.** which gives guidance on the use of personal digital assistants (PDA). See the last attachment of the publication, IC 2000-1, for the complete IC. A star (|) indicates revision from the last publication.

Chapter 1

GENERAL INFORMATION

1.1. Purpose. This instruction gives the directive requirements for the COMPUSEC component of the information assurance (IA) discipline as outlined in AFPD 33-2 and implements the Air Force COMPUSEC Program. This instruction applies to all Air Force military and civilian personnel and to Air Force contractors who develop, acquire, deliver, use, operate, or manage Air Force information systems.

1.2. Introduction. COMPUSEC is one of the IA disciplines promulgated in AFPD 33-2. Compliance assures measures are taken to protect all Air Force information system resources and information effectively and efficiently. Appropriate levels of protection against threats and vulnerabilities for information systems prevent denial of service, corruption, compromise, fraud, waste, and abuse.

1.3. Applicability. More restrictive DoDD and Director of Central Intelligence Agency directive requirements governing Special Category information or Special Access Program information take precedence over this.

1.4. Objectives. The objectives of COMPUSEC are to protect and maintain the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle. (**NOTE:** Authenticity and nonrepudiation are security services achieved by implementing accountability.) Use countermeasures to achieve the four objectives. Each safeguard and its associated control constitute a countermeasure. Security disciplines such as COMPUSEC, information security, emissions security, communications security (COMSEC), etc., provide safeguards to protect information. Controls are those administrative and management activities that implement the safeguards.

1.5. Information System Controls. Information system controls ensure the mission is accomplished in an effective and efficient manner and that changes to the information system or its environment do not affect mission readiness (see AFI 65-201, *Management Control*, and OMB Circular A-130). The following duties outline COMPUSEC responsibilities to ensure such readiness:

1.5.1. Designated Approving Authority (DAA):

1.5.1.1. Has the overall responsibility for the secure operation of the information system.

1.5.1.2. Makes appropriate decisions to balance security requirements, mission, and resources against the defined or perceived threat.

1.5.1.3. Has the resources to expend in support of the certification and security countermeasures.

1.5.2. Computer Systems Manager (CSM). The CSM is the individual operationally and administratively responsible for the proper functioning of the information system. Normally this is the senior communications officer in charge of a network or information system. CSMs plan and program budgetary, manpower, and training support for the operation and security of the system. They also develop administrative procedures (controls) to ensure the secure operation of the system. Duties include establishing accountability controls for IA, user training, measuring incidents, reporting; coordinating with the computer system security officer (CSSO); and identifying deficiencies. The CSM also establishes reporting controls between the CSSO and the unit COMPUSEC manager.

1.5.3. CSSO. The CSSO manages the COMPUSEC Program for an information system.

1.5.3.1. CSSOs monitor information system activities to ensure system integrity; establish reaction and maintenance controls for the facility; and perform system access or revocation tasks.

1.5.3.2. CSSOs continually identify threats, deficiencies, and associated countermeasures.

1.5.3.3. CSSOs measure and report incidents.

1.5.3.4. CSSOs ensure that the information system is operated, maintained, and disposed of according to security policies and practices.

1.5.4. COMPUSEC Manager. The unit COMPUSEC manager (typically the lead CSSO) establishes unit standardization and reporting controls as specified by the DAA and implements a unit COMPUSEC program to ensure compliance with the provisions of this instruction, including any major command (MAJCOM) or wing supplements.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Headquarters Air Force Communications and Information Center. HQ AFCIC/SY manages the Air Force COMPUSEC Program.

2.2. Headquarters Air Force Communications Agency.

2.2.1. Reviews, evaluates, and interprets national and DoD COMPUSEC policy and doctrine, and makes recommendations on implementation to HQ AFCIC/SY.

2.2.2. Develops, coordinates, and maintains HQ USAF/SC-approved Air Force COMPUSEC instructions, manuals, and pamphlets.

2.2.3. Develops, coordinates, publishes, and maintains HQ AFCIC/SY-coordinated specialized COMPUSEC publications.

2.2.4. Provides guidance and support to MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) in developing, implementing, and managing their COMPUSEC programs.

2.2.5. Manages the process of assessing government-produced and commercial-off-the-shelf software and hardware subsystem security features.

2.2.6. Develops security techniques and procedures with Air Force-wide applicability, coordinates the information with HQ AFCIC/SY, and distributes this information to MAJCOMs.

2.2.7. Processes waiver or deviation requests to Air Force COMPUSEC policy and instructions.

2.3. Headquarters Air Intelligence Agency (HQ AIA). Provides guidance concerning security requirements and implementation of information systems in Sensitive Compartmented Information facilities.

2.4. Air Force Information Warfare Center (AFIWC).

2.4.1. Collects and analyzes technical vulnerability information. Develops countermeasures or requests assistance from appropriate agencies. Advises Air Force users on appropriate countermeasures.

2.4.2. Obtains and distributes IA threat and vulnerability information to appropriate users.

2.4.3. Assists Air Force organizations in evaluating information systems security, recommending IA countermeasures, developing IA requirements documents, and advocating funding for IA research and development programs.

2.4.4. Maintains a database of COMPUSEC information reported by Air Force organizations and sends copies of the reports to all affected Air Force organizations.

2.5. Headquarters Air Force Materiel Command (HQ AFMC).

2.5.1. Assists HQ AFCA in developing COMPUSEC guidance and procedures for information systems in the acquisition and development life cycle.

2.5.2. Establishes IA training for single managers.

2.5.3. The Single Manager:

2.5.3.1. Ensures information systems they acquire and develop comply with COMPUSEC policies.

2.5.3.2. Develops a certification and accreditation (C&A) plan and documents it in the system security management plan.

2.5.3.3. Certifies and accredits information systems according to Air Force Systems Security Instruction 5024, Volume I (AFSSI 5024VI), *The Certification and Accreditation (C&A) Process*; AFSSI 5024VII, *The Certifying Official's Handbook*; AFSSI5024VIII, *The Designated Approving Authority's Handbook* (when published); and AFSSI 5024VIV, *Type Accreditation* (when published).

2.5.3.4. Continuously identifies and analyzes threats and vulnerabilities to the information system and its information to maintain an appropriate level of protection.

2.5.3.5. Ensures design reviews address information system security requirements.

2.5.3.6. Establishes security controls that protect the information system during development.

2.5.3.7. Ensures information system life-cycle responsibilities are documented. This includes responsibility for reaccomplishing risk analysis, security testing, and certification due to modifications or changes to the system.

2.5.3.8. Ensures operating agencies receive all security-related documentation (mission needs statement, operational requirements document, design reviews, hardware and software certifications, risk analysis, test and evaluation, trusted facility manual, security features users guide, etc.).

2.5.3.9. Ensures the information system documentation defines security procedures for system users, administrators, and maintainers.

2.5.3.10. Addresses all security-related issues to the systems security working group (see AFI 31-702, *System Security Engineering*).

2.6. Other Agencies Acquiring or Developing Information Systems or Software. Assume single manager responsibilities (paragraph **2.5.2.**) when they develop systems or software outside a program management office structure.

2.7. Designated Approving Authority:

2.7.1. Allocates funding and manpower resources to achieve and maintain an appropriate level of protection and to remedy security deficiencies.

2.7.2. As necessary, appoints a DAA representative to deal with the day-to-day issues of accrediting information systems according to AFSSI 5024VI.

2.7.3. Identifies CSSOs for all information systems under the DAA's jurisdiction.

2.7.4. Ensures IA personnel review all information system requirements documents to ensure IA requirements are appropriately addressed.

2.7.5. Appoints a certifying official to accomplish information system certification. Makes sure this individual possesses the technical expertise on the information system being certified and on the security mechanisms in use. The certifying official will not be in the wing or MAJCOM IA office.

2.8. Certifying Official:

2.8.1. Coordinates information system certification activities and tasks according to AFSSI 5024VII.

2.8.2. Leads certification teams formed to certify complex or large networks.

2.8.3. Based on system certification, makes technical judgments of an information system's compliance with the systems security policy, and develops an accreditation recommendation for submission to the DAA.

2.9. Major Commands. MAJCOMs implement and manage a COMPUSEC program throughout the command. FOAs and DRUs that elect to manage their own programs must document that in a support agreement according to AFI 25-201, *Support Agreements Procedures.*

2.9.1. MAJCOM IA Office. Implements and oversees the MAJCOM COMPUSEC program.

2.9.1.1. Sends copies of any command supplements to Air Force COMPUSEC instructions and policies to HQ AFCA/GCI and HQ AFCA/XPXP.

2.9.1.2. Assists subordinate units in developing their COMPUSEC programs.

2.9.1.3. Ensures communications and information system requirements documents include appropriate COMPUSEC requirements.

2.9.1.4. Reviews audit, vulnerability, and security survey reports for applicability within the command. Implements measures to correct deficiencies.

2.9.1.5. Ensures a feedback loop exists to comply with vulnerability and incident reporting and implementation of Air Force Computer Emergency Response Team (AFCERT) advisories according to AFSSI 5021, *Vulnerability and Incident Reporting*.

2.9.1.6. Ensures controls are in place to collect information system accreditation metric data according to AFI 33-205, *Information Protection Metrics and Measurements Program*.

2.9.1.7. Designates a single focal point to track and ensure MAJCOM compliance with C&A requirements for both classified and unclassified systems. The MAJCOM focal point acts as the single voice to the Defense Information Systems Agency (DISA) for the command regarding the Secret Internet Protocol Router Network (SIPRNET) C&A packages.

2.10. Wings. Establish a base-wide COMPUSEC program administered by the wing IA office. Obtain assistance and guidance from the wing IA office for IA requirements, technical solutions, and implementation.

2.10.1. Wing IA Office:

2.10.1.1. Assists the wing communications and information systems officer (CSO) and all base organizations and tenants in the development and management of their COMPUSEC programs.

2.10.1.2. Designates a single focal point to track and ensure wing and tenant unit compliance with C&A requirements for both classified and unclassified information systems. Identifies non-compliant systems and get-well dates. Provides information to local network control center (NCC) and MAJCOM IA office.

2.10.1.3. Routinely verifies with the NCC that only accredited systems (classified and unclassified) are connected to the base network.

2.10.1.4. Reviews information system certification documentation, and provides accreditation guidance and advice to DAAs within the wing based on this review.

2.10.1.5. Ensures information system requirements documents include appropriate COMPUSEC requirements.

2.10.1.6. Sends copies of any base supplements to Air Force COMPUSEC instructions and policies to their respective MAJCOMs.

2.10.1.7. Ensures a feedback loop exists to comply with vulnerability and incident reporting, and implementation of AFCERT advisories according to AFSSI 5021.

2.10.2. NCC. The NCC manages the local infrastructure that provides customers the communications and information resources needed to achieve their operational objectives. Consult AFI 33-115V1, *Network Management*, and AFSSI 5027, *Network Security Policy*, for detailed descriptions of the IA roles performed at the NCC by network managers, information protection operators, system administrators, help desk technicians, and workgroup managers.

2.11. Organizations. Commanders designate a unit COMPUSEC manager to oversee their COMPUSEC program. Unless required by the MAJCOM or wing, official designation of CSSOs is at the discretion of the unit COMPUSEC manager. If the CSSO positions are not assigned, their responsibilities reside with the unit COMPUSEC manager.

2.11.1. Unit COMPUSEC Manager:

2.11.1.1. Implements a unit COMPUSEC program to ensure compliance with the provisions of this instruction, including any MAJCOM or wing supplements.

2.11.1.2. Is the single liaison between the unit and the wing IA office for COMPUSEC matters.

2.11.1.3. Ensures all users and IA personnel receive training.

2.11.1.4. Establishes unit standardization and reporting controls for the unit as specified by the DAA.

2.11.1.5. Assigns CSSOs on a functional area or system-by-system basis.

2.11.2. Computer Systems Manager (CSM):

2.11.2.1. Determines the sensitivity level of the information and the criticality of information system resources and information.

2.11.2.2. Identifies information ownership for each multi-user information system to include accountability, access rights, and special handling requirements.

2.11.2.3. Establishes restrictions on shared usage of programs or files.

2.11.2.4. Obtains accreditation for information systems before operational use.

2.11.2.5. Ensures each information system operates within the constraints of the system security policy.

2.11.2.6. Plans and programs budgetary, manpower, and training support for the implementation and continuation of the COMPUSEC program to include improvements to security.

2.11.2.7. Ensures measures exist to control access to information systems based on users validated clearances, access approval for categories, and need to know.

2.11.2.8. Maintains information systems processing sensitive, classified, and critical information according to configuration management controls, and provides security guidance to the established configuration control board (CCB).

2.11.2.9. Provides information system security guidance to the data automation planner during the development of contingency plans for mission-critical and mission-essential systems.

2.11.2.10. Ensures appropriate classification guidance (e.g., security classification guide or derivative security classification guidance) is developed and made available to system security personnel prior to accreditation of information systems that process classified information or unclassified/sensitive information that may be classified in the aggregate.

2.11.3. CSSO. Workgroup managers (WM) may perform some or all of the duties listed below:

2.11.3.1. Establishes controls to ensure users operate, maintain, and dispose of information systems according to existing policy and procedures, including the system security policy.

2.11.3.2. Ensures procedures are in place for users to notify the CSSO or alternate if problems arise during critical or classified processing.

2.11.3.3. Ensures the system security policy for each information system is distributed to system users.

2.11.3.4. Establishes controls that ensure audit trails are periodically reviewed.

2.11.3.5. Performs an initial evaluation of each vulnerability or incident, and begins corrective or protective measures and reports according to AFSSI 5021.

2.11.3.6. Evaluates known vulnerabilities to ascertain if additional safeguards are needed to protect information systems.

2.11.3.7. Ensures all network and system administrators are taking aggressive action to implement AFCERT advisories and comply with the vulnerability and incident reporting procedures according to AFSSI 5021.

2.11.3.8. Ensures users receive training on system-specific security procedures, and informs network and system administrators to frequently check vendor sources for information regarding vulnerabilities for their particular hardware and software.

2.11.3.9. Periodically validates user-access privilege levels.

2.11.3.10. Maintains the accreditation according to AFSSI 5024VI.

2.11.3.11. Provides C&A information to the wing IA office for appropriate tracking.

2.11.3.12. Ensures organizations do not use shareware or public domain software until approved for use by the DAA. The CSSO must ensure the software is free of viruses, hidden defects, and obvious copyright infringements. The CSSO or WM perform testing.

2.11.4. Users:

2.11.4.1. Protect system information and resources according to established security policies and procedures and Air Force Systems Security Memorandum (AFSSM) 5019, *Computer Security Users Guide*.

2.11.4.2. Report system security incidents, vulnerabilities, and virus attacks according to AFSSI 5021.

Chapter 3

MINIMUM REQUIREMENTS

3.1. General. Safeguard computer systems and information against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons. Protect hardware, firmware, software, and information against unauthorized disclosure, destruction, or modification.

3.1.1. Prior to operating, certify and accredit all information systems according to AFSSI 5024VI and AFSSI 5024VII.

3.1.2. Recertify and reaccredit all information systems every 3 years unless changes to the information system or environment baseline impact security, thereby necessitating recertification or reaccreditation sooner.

3.1.3. Implement a minimum of Class 2 (C2) functionality according to AFMAN 33-229, *Controlled Access Protection (CAP)*. (**NOTE:** C2, as used in this instruction, indicates the criteria class [controlled access protection] represented in DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985, and not command and control.)

3.1.4. Information systems whose life span extends beyond 1999 must have countermeasures in place to correct the Year 2000 (Y2K) vulnerability. Test for this vulnerability during system C&A. If the Y2K vulnerability has not been countered, it must be reported as a residual risk in the risk analysis report.

3.2. Designated Approving Authority Assignment.

3.2.1. The wing commander is the DAA for the base-wide area or metropolitan area network and for all networks owned and/or operated by the wing.

3.2.1.1. The wing commander may delegate DAA authority to each operational or support commander for his or her systems and networks. Further delegation is prohibited.

3.2.1.2. The wing commander may delegate DAA authority to the ranking officer at each geographically separated organization for his or her systems and networks. Further delegation is prohibited.

3.2.2. MAJCOM, FOA, DRU, and tenant unit commanders are DAAs for the systems and networks they own and/or operate.

3.2.2.1. MAJCOM, FOA, DRU, and tenant unit commanders may, if appropriate, delegate the authority to the wing commander, to a single headquarters director (i.e., 2-letter office symbol), or each operational support commander for his or her systems and networks. Further delegation is prohibited.

3.2.2.2. MAJCOM, FOA, DRU, and tenant unit commanders may delegate DAA authority to the ranking officer at each geographically separated entity (i.e., detachment, organization, center, unit, etc.). Further delegation is prohibited.

3.2.3. Agencies that direct the acquisition, development, fielding, and/or sustainment of a specific system ensure a DAA is appointed. DAA appointments (i.e., due to lead command responsibilities, joint or Air Force standard system, etc.) must be consistent with the above policy. For example, if Air

Combat Command (ACC) is the lead command for a logistics standard system, the appropriate DAA would be HQ ACC/LG, or its lead agency.

3.3. Controlled Access Protection Products.

3.3.1. Use computer-based security features to satisfy security requirements for information systems. Where computer-based security is not feasible, enhance existing safeguards and controls to satisfy security requirements according to AFMAN 33-229.

3.3.2. Evaluate, assess, or locally test and approve all hardware, software, and firmware products that provide security features prior to use on any accredited information system or network. Implement computer-based security solutions in the following order:

3.3.2.1. Use products evaluated by the National Computer Security Center (NCSC) listed on the Evaluated Products List.

3.3.2.2. Use products formally assessed by HQ AFCA listed on the Assessed Products List.

3.3.2.3. Select a suitable product, then test and certify its security features according to AFSSI 5024VII. Certification must validate claims that the security features meet Air Force and DoD security policy or that additional countermeasures are required.

3.4. Software Security.

3.4.1. Certify all software prior to installation and use on an operational accredited system. Follow the software certification process outlined in AFSSI 5024VI and ensure DAA approval is granted. (**NOTE:** Freeware, public domain software, and shareware originating from questionable or unknown sources, [e.g., non-DoD bulletin boards or World Wide Web sites, etc.] are much more susceptible to malicious logic and may violate the system security policy. Base use of such software on operational need.)

3.4.2. Avoid software development, testing, and debugging on operational information systems. If no alternate exists, meet the following conditions:

3.4.2.1. Protect applications and files from unauthorized disclosure.

3.4.2.2. Maintain the availability, confidentiality, integrity, and accountability of information system resources and information.

3.5. Personal Computers (PC) and Workstations. This section applies to all information systems used by only one individual at a time. The PC or workstation may be operated as a stand-alone system or connected in a network environment. (**NOTE:** Information systems that allow file sharing over a network must comply with the requirements of multi-user information systems [paragraph **3.6.**].)

3.5.1. Unclassified and Sensitive Processing:

3.5.1.1. Verify each user's need for access to information system resources and information. Follow identification and authentication procedures according to AFMAN 33-223, *Identification and Authentication*.

3.5.1.2. Confirm that information systems added to the network comply with the system security policy.

3.5.1.3. Protect against casual viewing of information by using password-protected screen savers when workstations are unattended.

3.5.1.4. Protect the information system and data against tampering. Provide protection from outsider threats by controlling physical access to the information system itself. Provide protection from insider and outsider threats by installing keyboard locks, basic input/output system (BIOS) passwords, password-protected screen savers, add-on security software, etc., or by establishing controls for removal and secure storage of information from unattended information systems. (**NOTE:** Using password-protected screen savers in conjunction with BIOS passwords affords maximum protection for sensitive information. Using screen saver alone provides minimal protection.)

3.5.1.5. Protect against unauthorized web browser access. Use protection measures in paragraph **3.5.1.4.** and use dynamic host Internet protocol addressing or local operating system security features to force each workstation to log onto the network before granting web access.

3.5.1.5.1. Disable ActiveX and Java features when visiting untrusted sites (non-.gov or -.mil sites). When mission accomplishment necessitates the need to enable these features, obtain DAA approval and update C&A documentation.

3.5.1.6. Clear or destroy media used to store sensitive information before release to unauthorized personnel. Follow procedures in AFSSI 5020, *Remanence Security* (will convert to AFMAN 33-224).

3.5.1.7. Install vendor-produced system patches and implement procedural countermeasures according to AFCERT or Automated System Security Incident Support Team guidance immediately upon receipt. In the rare case where security-relevant system patches cannot be implemented, exceptions to implementing the remedies must be approved by the DAA and documented in the risk analysis. Send copies of approved exceptions and updated risk analysis to the MAJCOM IA office and command/SC (i.e., MAJCOM/SC, FOA/SC, DRU/SC).

3.5.2. Classified Processing. In addition to the security requirements in paragraph **3.5.1.**, the following security requirements apply:

3.5.2.1. Physically protect each network node to a level adequate for protecting the most restricted information accessible at the node.

3.5.2.2. Information systems using nonvolatile, nonremovable storage media must meet one of the following conditions:

3.5.2.2.1. Install the computer in an area approved for open storage of classified information at or above the highest classification level of the information processed.

3.5.2.2.2. Use an NCSC-evaluated, AFCA-assessed, or locally tested and DAA-approved product or technique to prevent storing classified information on nonvolatile, nonremovable storage media. Ensure product protects against inadvertently writing information to storage media.

3.5.2.3. Unless multi-level security (i.e., criteria class B) is implemented according to DoD 5200.28-STD, ensure all personnel authorized to use the information system are cleared to the highest level and most restricted category of information contained in the information system.

3.5.2.4. Use a separate copy of the operating system and other necessary software for each level of classification on information systems employing periods processing.

3.5.2.5. Clear equipment and media when changing modes of operation or changing operations to the same or higher classification level. Sanitize storage devices that contain classified information before using at a lower classification level according to AFSSI 5020.

3.5.2.6. Safeguard, mark, and label output products and removable media according to DoDD 5200.1, *DoD Information Security Program*, December 13, 1996; and AFI 31-401, *Information Security Program Management*.

3.5.2.7. Provide internal markings on files to indicate the information sensitivity level and any special handling instructions, where practical.

3.5.3. Guidance on the use of personal digital assistants (PDA):

3.5.3.1. A PDA is an automated information system and therefore is subject to Air Force policy and guidance governing the security and use of a desktop or notebook computer.

3.5.3.2. Use of PDAs (e.g., Palm Pilot® or Cassiopeia® devices) within the Air Force has increased significantly. This family of devices offers personal productivity enhancements, particularly by making certain features of the desktop environment portable (e.g., Microsoft Outlook® contacts, notes, appointments, and E-mail); however, the use of some products and features introduces security risks to information systems and networks.

3.5.3.3. Individuals may use PDAs to:

3.5.3.3.1. Process unclassified information from desktop workstations. This includes the following typical features: schedules, contact information, notes, E-mail, and other items.

3.5.3.3.2. Take notes, save information, or write E-mails, when away from desktop workstations, whether down the hall or out of the country.

3.5.3.3.3. Synchronize information with desktop workstations.

3.5.3.4. Do not use PDAs for the following:

3.5.3.4.1. Do not process or maintain classified information. There are currently no approved methods for clearing (sanitizing) classified information from these devices. If contaminated, security personnel must protect, confiscate, or possibly destroy the affected PDA.

3.5.3.4.2. Do not connect or subscribe to commercial internet service providers (ISP) for official E-mail services (e.g., Palmnet® wireless communications service). The use of commercial ISPs for official business is not allowed due to the high operational risk posed by the possible collection of sensitive information.

3.5.3.4.3. Do not synchronize information across a network using a wireless connection. The configuration required to permit this functionality introduces unacceptable risks into a network--opening firewall ports and sending passwords in the clear. Exceptions to this restriction will be evaluated on a case-by-case basis and require local DAA approval.

3.5.3.5. Software security restrictions described in paragraph **3.4.** apply to these devices.

3.5.3.6. The only authorized connection through a PDA modem is to an official Air Force remote access server (RAS) account protected by an authorized network control center firewall. Do not synchronize the PDA remotely by direct dial-in access to desktops.

3.5.3.7. Do not issue users a PDA until they agree, at a minimum, to the terms outlined in paragraph **3.5.3.**

3.5.3.8. You can find additional security related information on PDAs at the AFCA product evaluation webpage (http://www.afca.scott.af.mil/prodeval).

3.6. Multi-User Information Systems. This section applies to all multi-user file servers (e.g., file transfer protocol [FTP]), network file servers, World Wide Web servers, etc.), and information systems that permit file sharing, perform network security functions, or provide security services (e.g., Automated Security Incident Monitoring [ASIM], firewalls, etc.). AFI 33-115V1 directs that all communications and information services entering and exiting the base or site fall under the operational control of the NCC. Follow AFIWC and AFCA guidance on implementing network boundary protection to include the ASIM system, installing and configuring firewalls, and disabling system services (e.g., Barrier Reef “How to Guides”). AFSSI 5027 provides additional guidelines for securing computer networks.

3.6.1. Unclassified and Sensitive Processing. In addition to the security requirements listed in paragraph **3.5.1.**, the following security requirements apply. If conflicts develop, the following requirements take precedence:

3.6.1.1. Adhere to AFMAN 33-223 to ensure individual accountability and use of proper identification and authentication (I&A) procedures, and verify access.

3.6.1.2. Control access to files, software, and devices so that only authorized users can use them.

3.6.1.3. Control access to prevent unauthorized persons from using network facilities.

3.6.1.4. Use network components (e.g., trusted routers, bastion hosts, gateways, firewalls, etc.) or information systems that enforce mandatory access control and I&A to provide access controls.

3.6.1.5. Provide each user with only those system privileges needed for assigned tasks (least privilege concept).

3.6.1.6. Limit access to privileged programs (i.e., operating system, system parameter and configuration files, and databases), utilities (i.e., assemblers, debuggers, maintenance utilities), and security-relevant programs/data files (i.e., security monitor, password files, and audit files) to authorized personnel (i.e., system administrator and CSSO).

3.6.1.7. Limit the capability to conduct privileged actions (i.e., loading new users, password management, modifying and patching system routines or files, examining memory locations, real-time monitoring of user activities, and initiating or executing privileged routines) to authorized personnel.

3.6.1.8. Implement auditing according to AFMAN 33-229 for C2 criteria class information systems. Information systems operating at higher criteria classes will implement audit requirements according to DoDD 5200.28-STD.

3.6.1.8.1. Establish an audit record capable of tracing network activity and actions to an individual user.

3.6.1.8.2. Ensure the audit mechanism records any event that attempts to change the security profile (e.g., access controls, security level of the subject, user password, etc.).

3.6.1.8.3. When technically feasible, ensure the information system aborts or suspends unauthorized user activity when detected, unless performing real-time analysis.

3.6.1.9. Generate output only within the central facility or at a remote station staffed with personnel cleared for the highest sensitivity level of information processed by the information system when the system does not have controls that limit output to authorized users.

3.6.1.10. Implement normal building and area entry controls (i.e., physical, administrative, and personnel security) at remote terminal sites when host systems have adequate internal access controls. Disable communications lines and take other necessary actions to protect information, systems, and resources when adequate internal controls do not exist.

3.6.1.11. Protect transmissions of classified, sensitive, or a combination of classified and sensitive information according to AFSSI 4100VI, (FOUO) *The Air Force Communications Security (COMSEC) Program*.

3.6.2. Classified Processing. In addition to the security requirements listed in paragraph **3.5.** and paragraph **3.6.1.**, the following security requirements apply. If conflicts develop, the following requirements take precedence:

3.6.2.1. Where the facility (building and room) plays a major role in providing security for information systems, establish procedures to notify IA personnel of impending changes to the facility.

3.6.2.2. Operate networks in a system high or dedicated security mode unless all network nodes are accredited for operation in the multilevel or partitioned security mode.

3.6.2.3. Adhere to the DISA Connection Approval Process if the system is connected to SIPRNET.

3.6.2.4. Use only Secret and Below Interoperability (SABI)-approved devices and adhere to SABI configuration guidelines when connecting classified systems or networks to unclassified systems or networks.

3.7. Foreign National Access to Air Force Information Systems . USAF/CVA is responsible for authorizing foreign national access to information systems operated by HQ USAF, DRUs, and Secretary of the Air Force (SAF) functionals. USAF/CVA may further delegate authority to HQ USAF Deputy Chiefs of Staff, AFCIC/CC, and the USAFA Superintendent. Authorizing access to SAF-operated systems is delegated to the SAF assistant secretary level. Delegating authority for these positions shall not occur below the three-star level. MAJCOM commanders (MAJCOM/CC) are responsible for authorizing foreign national access to information systems within their respective commands. Delegating authority shall not occur below the MAJCOM vice commander.

3.7.1. Before authorizing foreign national access to specific information contained within an information system, the designees will:

3.7.1.1. Ensure the information is properly processed for disclosure.

3.7.1.2. Ensure systems accreditation authorities concur with the access.

3.7.1.3. Ensure the C&A documentation for the system is updated to reflect foreign national access.

3.7.1.4. Ensure security measures employed adhere to information assurance policy.

3.7.2. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6740.01, *Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations*, 18 September 1996, directs establishing a memorandum of agreement between the United States and the foreign nation requiring use of the Defense Information Systems Network (DISN) prior to providing the foreign national telecommunications service, such as access to United States information systems. This agreement must clearly define all obligations and benefits concerning military communications support and related supplies and services provided and the mechanism for reimbursement of costs.

3.7.3. CJCSI 6211.02A, *Defense Information System Network and Connected Systems*, 22 May 1996 identifies the Joint Staff/J6 Director as the responsible agent for DISN operational network policy. The instruction also requires the DISA Director to establish and publish DISN connection requirements. Authority to connect to the DISN-SIPRNET, DISN-Nonsecure Internet Protocol Router Network (NIPRNET), or other networks by foreign entities does not equate to authority to exchange data or access systems located on that network. The DAA or designated release/disclosure authority, grants access to information and information systems. Ensure authorization is pursuant to a written arrangement concluded in accordance with applicable instructions enabling access to the information. Submit requirements to your MAJCOM foreign disclosure office and other appropriate offices (i.e., MAJCOM IA office, personnel security, DAA, etc.) for proper processing before seeking service, commander-in-chief (CINC), and/or Joint Staff/J6 approval.

3.7.4. The United States Military Communications-Electronics Board establishes DISN connection requirements for information systems connecting to the DISN-SIPRNET requiring access by foreign nationals.

3.7.4.1. The service sponsor and authority responsible for granting foreign national access to Air Force information systems shall request Joint Staff/J6 approval in order to connect to DISN-SIPRNET. For Air Force information systems requiring DISN-SIPRNET access that support a CINC, the sponsoring CINC for the foreign national requests Joint Staff approval. Furthermore, the request must include items identified in the draft DISA Connection Approval Process (see AFCA Home Page)(i.e., mission statement, organizations involved, and points of contact [POC], brief description of current environment to include topology, consent-to-monitor statement, etc.). DISA, the National Security Agency, the CINC, and/or service representatives engineer a technical solution through the SABI process upon validation of the requirement by Joint Staff/J6. The technical solution must include a high assurance guard in United States-controlled space to protect United States-only information and information systems. The functional user must submit C&A documentation to DISA and present the technical solution to the DISN Security Accreditation Working Group (DSAWG). If approved, the DSAWG advises the sponsoring CINC and/or service and DISA, in writing, so DISA can grant the approval to connect.

3.7.5. For DISN-NIPRNET access, the appropriate sponsor (CINC, USAF/CVA, or MAJCOM/CC) sends service-validated requirements to the Joint Staff/J6 for approval. The request must contain the following information from the system C&A documentation: a brief mission statement and description of current environment, organizations involved and POCs, type of connectivity required (e.g., HyperText Transfer Protocol, Simple Mail Transfer Protocol, FTP, etc.), what and how often information will be transmitted, releasability of information as determined by the MAJCOM foreign disclosure office, and a copy of the accreditation statement by the local DAA. In addition, include a proposed solution that explains how access by the foreign national will be limited to only the information determined to be releasable by the appropriate foreign disclosure office (a high assurance guard is not a requirement for NIPRNET access).

3.7.6. Connection by stand-alone systems or networks within a local enclave or through means other than the DISN requires approval by the MAJCOM/CC or USAF/CVA. Coordinate requests through appropriate offices and include complete C&A documentation according to AFSSI 5024VI.

3.7.7. For all Air Force systems accessing the DISN-SIPRNET or DISN-NIPRNET, get appropriate service coordination and service authorization before proceeding with CINC coordination and/or Joint Staff approval.

3.8. Configuration Management.

3.8.1. Use configuration management to ensure the integrity of critical functions in security-related hardware, firmware, and software of all information systems. Distributing hardware, firmware, and software under configuration management control shall be provided an appropriate level of protection to assure product integrity. Use the computer resources life-cycle management plan and the CCB to ensure system integrity throughout the life cycle of an information system.

3.8.2. Ensure interoperability and compatibility with existing Air Force standard network security policies and procedures according to the Joint Technical Architecture-Air Force.

3.9. Remote Access via Modem.

3.9.1. Centralize modem management under the NCC according to AFSSI 5027. Do not use modems in any PC or laptop computer while physically connected to the base network. Stand-alone PCs may use modems when approved by the DAA (i.e., Bulletin Board).

3.9.2. The security requirements (e.g., I&A, audit, etc.) of the local information system also apply to systems allowed to remotely access that information system.

3.9.3. Make sure that access tables, when used, remain current.

3.9.4. Prohibit the use of call-forwarding capabilities when using callback or dialback technology.

3.9.5. Annotate remote access in the audit logs.

3.9.6. Do not publicize telephone numbers to anyone other than those with a need to know.

3.9.7. Employ methods for controlling access (e.g., callback, token generation, etc.) where the capability exists.

3.10. Using Hardware or Software Not Owned by the Air Force.

3.10.1. Contractor-Owned. Contractor-owned or -operated hardware and software must meet all security requirements for government-owned hardware and software. AFI 31-601, *Industrial Security Program Management*, provides security policy and guidance relating to contractor actions involving classified information. DoD Manual 5220.22 (DoD 5220.22-M), *National Industrial Security Program Operating Manual*, January 1995, applies to off-base contractor information systems and on-base contractor facilities when the Air Force does not have responsibility for industrial security inspections. If DoD 5220.22-M applies, Defense Investigative Service approval is mandatory before processing classified information. If the contractor must comply with this instruction instead of the manual, the Air Force must provide the contractor with specifications that establish contractor and Air Force responsibilities for security, including who should conduct the information system C&A and who the DAA is for the system. The program or project manager, contracting or procurement officer, and appropriate COMPUSEC personnel should jointly develop this guidance.

3.10.2. Other Service or Agency Owned (**NOTE:** Where a lead service is other than the Air Force, some protection requirements may not be achievable). Develop an agreement before using equipment and facilities owned or operated by other services or agencies to ensure:

3.10.2.1. Air Force use of other services' or agencies' resources does not degrade the required security posture.

3.10.2.2. Mission-critical processing takes priority.

3.10.2.3. The lead service (in joint-service activities) identifies the DAA for the information system and determines security requirements for the information systems supporting the activity.

3.10.2.4. Satisfying Air Force requirements in this instruction for the protection of Air Force information.

3.10.3. Foreign Owned. Do not use foreign-owned or -operated (e.g., joint/coalition) information systems to process sensitive or classified information or for critical processing, unless required by international treaties or security agreements.

3.10.4. Personally Owned. Do not use personally owned hardware or software to process classified information. Using personally owned hardware and software for government work is strongly discouraged; however, it may be used for processing unclassified and sensitive information with DAA approval (see AFI 33-112, *Computer Systems Management*; and AFI 33-114, *Software Management*). (**NOTE:** Document blanket approvals for the purpose of telecommuting in a local operating instruction.) Base approval on the following requirements:

3.10.4.1. The written approval specifies the conditions under which the information system operates.

3.10.4.2. When using a personally owned information system for official work, the system must employ anti-virus software, government-owned sensitive information must remain on removable media, and government-owned sensitive information must be marked and protected according to the sensitive category (e.g., Privacy Act, For Official Use Only [FOUO], etc.) program directives.

3.11. Controlling Maintenance Activities.

3.11.1. Restrict information system maintenance to authorized personnel with a security clearance for the highest classification and most restricted category of information processed. Uncleared individuals may perform maintenance on information systems used to process classified information only if the information is purged or an appropriately cleared individual (capable of identifying unauthorized activity) observes their actions.

3.11.2. Allow remote software diagnostics or maintenance only if the information system audits such activities or an appropriately cleared individual (capable of identifying unauthorized activity) observes such activities. When maintenance activities are suspended or completed, disconnect or disable access to the information system. Additionally, verify the identity of the maintenance personnel to prevent the unauthorized disclosure of sensitive and classified information.

3.11.3. Prevent vendor maintenance personnel from removing classified or sensitive media, products, etc., from government facilities when those personnel do not have the proper authorization (e.g., verified identity, security clearance, access approval for categories, need to know) to access that media. Before releasing an information system component containing nonvolatile storage media (e.g., tapes, disks, battery-powered random access memory, etc.) to uncleared maintenance activities, sanitize the component of classified and/or sensitive information according to AFSSI 5020.

3.12. Computer Security Documentation. Information system requirements documents must specify security requirements. Acquiring agencies will develop security-related documentation and deliver to the customer along with the information system.

3.13. Malicious Logic Protection. Protect information systems (including network servers) from malicious logic (e.g., virus, worm, Trojan horse, etc.) attacks. Apply an appropriate mix of preventive measures to include user awareness training, local policies, configuration management, and anti-virus software. At a minimum:

3.13.1. Implement anti-virus software on all information systems and networks.

3.13.2. Where feasible, scan all incoming traffic and files for viruses at the network server level.

3.13.3. Scan removable media for viruses before each use. Scan fixed media daily.

3.13.4. Report all virus attacks according to AFSSI 5021.

3.13.5. Use anti-virus software available through DoD channels. Forward waiver requests to HQ AFCA/GCI for approval or disapproval.

3.13.6. Establish procedures to rapidly obtain, distribute, and install changes to anti-virus software on all information systems (including network servers).

3.13.7. Preserve malicious logic reports as evidence for ongoing investigations.

3.13.8. Include virus prevention, detection, eradication, and reporting procedures in user awareness training.

3.14. Information Assurance Security Awareness, Training, and Education (SATE). All Air Force personnel will receive IA awareness, training, and education throughout their assignments according to AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*.

3.15. Notice and Consent for Information System Monitoring. Information systems are subject to monitoring by authorized personnel. Display warning banners according to AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*.

3.16. Reporting:

3.16.1. Report information system accreditation according to AFI 33-205.

3.16.2. Report information system vulnerabilities, security incidents, and virus attacks according to AFSSI 5021.

JOHN L. WOODWARD, JR., Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSI 6211.02A, *Defense Information System Network and Connected Systems*, 22 May 1996

CJCSI 6740.01, *Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations,* 18 September 1996

Information Technology Management Reform Act (ITMRA) of 1996

DoDD 5200.1, *DoD Information Security Program, December 13, 1996*

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs),* March 21, 1988

DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985 (commonly referred to as the Orange Book)

DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995

DoD 7740.1-G, *Department of Defense ADP Internal Control Guideline,* July 1998

OMB Circular A-130, *Management of Federal Information Resources*

OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994 as amended through 7 December 1998

P.L. 100-235, *Computer Security Act of 1987*

Title 5 U.S.C. Section 552a (Privacy Act)

AFI 25-201, *Support Agreements Procedures*

AFI 31-401, *Information Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 31-702, *System Security Engineering*

AFPD 33-2, *Information Protection*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-115V1, *Network Management*

AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*

AFI 33-205, *Information Protection Metrics and Measurements Program*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFMAN 33-223, *Identification and Authentication*

AFMAN 33-229, *Controlled Access Protection (CAP)*

AFI 65-201, *Management Control*

AFDIR 33-303, Compendium of Communications and Information Technology

AFSSI 4100VI, (FOUO) *The Air Force Communications Security (COMSEC) Program*

AFSSM 5019, *Computer Security Users Guide*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Vulnerability and Incident Reporting*

AFSSI 5024VI, *The Certification and Accreditation (C&A) Process*

AFSSI 5024VII, *The Certifying Official's Handbook*

AFSSI 5024VIII, *The Designated Approving Authority's Handbook* (when published)

AFSSI 5024VIV, *Type Accreditation* (when published)

AFSSI 5027, *Network Security Policy*

Abbreviations and Acronyms

ACC—Air Combat Command

ADP—Automated Data Processing

AFCA—Air Force Communications Agency

AFCERT—Air Force Computer Emergency Response Team

AFCIC—Air Force Communications and Information Center

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force Manual

AIA—Air Intelligence Agency

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Memorandum

ASIM—Automated Security Incident Monitoring

BIOS—Basic Input/Output System

C2—Class 2 (Controlled Access Protection)(a division and class of DoD 5200.28-STD

C&A—Certification and Accreditation

CCB—Configuration Control Board

CINC—Commander-in-Chief

CIO—Chief Information Officer

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

COMPUSEC—Computer Security

COMSEC—Communications Security

CSM—Computer Systems Manager

CSO—Communications and Information Systems Officer

CSSO—Computer System Security Officer

DAA—Designated Approving Authority

DAC—Discretionary Access Control

DISA—Defense Information Systems Agency

DISN—Defense Information Systems Network

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

DSAWG—DISN Security Accreditation Working Group

FOA—Field Operating Agency

FOUO—For Official Use Only

FTP—File Transfer Protocol

IA—Information Assurance

I&A—Identification and Authentication

IP—Information Protection

ITMRA—Information Technology Management Reform Act

JP—Joint Publication

MAC—Mandatory Access Control

MAJCOM—Major Command

NATO—North Atlantic Treaty Organization

NCC—Network Control Center

NCSC—National Computer Security Center

NIPRNET—Non-Secure Internet Protocol Router Network

OMB—Office of Management and Budget

PC—Personal Computer

P.L.—Public Law

POC—Point of Contact

SABI—Secret and Below Interoperability

SAF—Secretary of the Air Force

SATE—Security Awareness, Training, and Education

SIPRNET—Secret Internet Protocol Router Network

WM—Workgroup Manager

Y2K—Year 2000

Terms

Accountability—1. Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation. 2. (DoD) The obligation imposed by law or lawful order or regulation on an officer or other person for keeping accurate records of property, documents, or funds. The person having this obligation may or may not have actual possession of the property, documents, or funds. Accountability is concerned primarily with records while responsibility is concerned primarily with custody, care, and safekeeping. (JP 1-02)

Accreditation—1. Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls. 2. (DoD) In computer modeling and simulation, an official determination that a model or simulation is acceptable for a specific purpose. (JP 1-02)

Authenticity—Measure of the confidence that the security features and architecture of an information system accurately mediate and enforce the system security policy.

Category—A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented information.

Certification—Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certifying Official—Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

Communications and Information Systems Officer (CSO)—At base level, the commander of the communications unit responsible for carrying out communications and information systems responsibilities. At MAJCOM, the person designated by the MAJCOM/CC responsible for overall management of communications and information systems budgeted and funded by that command. When no other office is formally designated as chief information officer (CIO), the CSO ensures compliance with the mandates of the Information Technology Management Reform Act (ITMRA) of 1996.

Computer-Based Security—Security for the information system is provided through the use of automated security features.

Computer Systems Manager (CSM)—Official with supervisory or management responsibility for an organization, activity, or functional area that owns or operates an information system. They are operationally and administratively responsible for the mission that the information system supports. They are responsible for the security-related functions within their office or facilities. (**NOTE:** This is not an appointed position. For office automation systems, the office chief or manager is normally the CSM.)

Computer Systems Security Officer (CSSO)—Official who manages the COMPUSEC program for an information system assigned to him or her by the CSM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices.

Confidentiality—The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls—Prescribed actions taken to maintain the appropriate level of protection for information systems. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of information system activities, or report incidents. (**NOTE:** There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DoD 7740.1-G, *Department of Defense ADP Internal Control* Guideline, July 1998, outlines internal controls for information systems.)

Countermeasures—1. The sum of a safeguard and its associated controls. 2. (DoD) That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Formal Access Approval—Documented approval by a data owner to allow access to a particular category of information.

Information—1. Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (**NOTE:** Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (JP 1-02) 3. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information System—1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (**NOTE:** This includes automated information systems.) 2. (DoD) The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

Integrity—Property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

Level of Protection—Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the information system.

Nonrepudiation—Method by which the sender of data is provided proof of delivery and the recipient is assured of the sender's identity so that neither can deny having processed the data.

Periods Processing—Processing of various levels of classified and unclassified information at distinctly different times. (**NOTE:** Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.)

Safeguards—Protective measures and controls prescribed to meet the security requirements of an information system. (**NOTE:** Safeguards include security features and management constraints from the various security disciplines [i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security] used in concert to provide the requisite level of protection.)

Security Feature—A hardware-, firmware-, or software-controlled access protection to meet the security requirements of I&A; mandatory access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system security safeguards.

Sensitive Information—Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (**NOTE:** Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

Stand-Alone System—An information system physically and electronically isolated from all other systems and intended to be used by one user at a time, with no data belonging to other users remaining on the system (e.g., a PC with removable storage media such as a floppy disk).

Standard System—Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

System Integrity—The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Security Policy—Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (**NOTE:** It interprets regulatory [e.g., DoDD 5200.28, AFPD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.)

Tampering—Unauthorized modification that alters the proper functioning of information system security equipment.

Threat—Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, fraud, waste, or abuse to a system.

User—Person or process accessing an information system by direct connections (e.g., via terminals) or indirect connections.

Vulnerability—1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 1-02) 3. (DoD) The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1-02)

Workgroup Manager (WM)—A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.

Attachment 2

IC 2000-1 TO AFI 33-202, COMPUTER SECURITY

22 JUNE 2000

This instruction implements the computer security (COMPUSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and establishes Air Force COMPUSEC requirements for information protection to comply with Public Law (P.L.) 100-235, *Computer Security Act of 1987*; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*; and Department of Defense Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AIS)*, March 21, 1988. You may use extracts from this Air Force instruction (AFI). Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITPP), 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCI, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5222, and HQ Air Force Communications and Information Center (HQ AFCIC/SYI), 1250 Air Force Pentagon, Washington DC 20330-1250. For a glossary of references and supporting information refer to **Attachment 1** and AFDIR 33-303, *Compendium of Communications and Information Technology*. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

Updates purpose paragraph to include trade name statement. Adds paragraph **3.5.3.** which gives guidance on the use of personal digital assistants (PDA). See the last attachment of the publication, IC 00-1, for the complete IC. A star (|) indicates revision from the last publication.

3.5.3. Guidance on the use of personal digital assistants (PDA):

3.5.3.1. A PDA is an automated information system and therefore is subject to Air Force policy and guidance governing the security and use of a desktop or notebook computer.

3.5.3.2. Use of PDAs (e.g., Palm Pilot® or Cassiopeia® devices) within the Air Force has increased significantly. This family of devices offers personal productivity enhancements, particularly by making certain features of the desktop environment portable (e.g., Microsoft Outlook® contacts, notes, appointments, and E-mail); however, the use of some products and features introduces security risks to information systems and networks.

3.5.3.3. Individuals may use PDAs to:

3.5.3.3.1. Process unclassified information from desktop workstations. This includes the following typical features: schedules, contact information, notes, E-mail, and other items.

3.5.3.3.2. Take notes, save information, or write E-mails, when away from desktop workstations, whether down the hall or out of the country.

3.5.3.3.3. Synchronize information with desktop workstations.

3.5.3.4. Do not use PDAs for the following:

3.5.3.4.1. Do not process or maintain classified information. There are currently no approved methods for clearing (sanitizing) classified information from these devices. If contaminated, security personnel must protect, confiscate, or possibly destroy the affected PDA.

3.5.3.4.2. Do not connect or subscribe to commercial internet service providers (ISP) for official E-mail services (e.g., Palmnet® wireless communications service). The use of commercial ISPs for official business is not allowed due to the high operational risk posed by the possible collection of sensitive information.

3.5.3.4.3. Do not synchronize information across a network using a wireless connection. The configuration required to permit this functionality introduces unacceptable risks into a network--opening firewall ports and sending passwords in the clear. Exceptions to this restriction will be evaluated on a case-by-case basis and require local DAA approval.

3.5.3.5. Software security restrictions described in paragraph **3.4.** apply to these devices.

3.5.3.6. The only authorized connection through a PDA modem is to an official Air Force remote access server (RAS) account protected by an authorized network control center firewall. Do not synchronize the PDA remotely by direct dial-in access to desktops.

3.5.3.7. Do not issue users a PDA until they agree, at a minimum, to the terms outlined in paragraph **3.5.3.**

3.5.3.8. You can find additional security related information on PDAs at the AFCA product evaluation webpage (http://www.afca.scott.af.mil/prodeval).

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSI 6211.02A, *Defense Information System Network and Connected Systems*, 22 May 1996

CJCSI 6740.01, *Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations*, 18 September 1996

Information Technology Management Reform Act (ITMRA) of 1996

DoDD 5200.1, *DoD Information Security Program, December 13, 1996*

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985 (commonly referred to as the Orange Book)

DoD 5220.22-M, *National Industrial Security Program Operating Manual*, January 1995

DoD 7740.1-G, *Department of Defense ADP Internal Control Guideline*, July 1998

OMB Circular A-130, *Management of Federal Information Resources*

OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994 as amended through 7 December 1998

P.L. 100-235, *Computer Security Act of 1987*

Title 5 U.S.C. Section 552a (Privacy Act)

AFI 25-201, *Support Agreements Procedures*

AFI 31-401, *Information Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 31-702, *System Security Engineering*

AFPD 33-2, *Information Protection*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-115V1, *Network Management*

AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*

AFI 33-205, *Information Protection Metrics and Measurements Program*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFMAN 33-223, *Identification and Authentication*

AFMAN 33-229, *Controlled Access Protection (CAP)*

DELETE AFMAN 33-270, Command, Control, Communications, and Computer (C4) Systems Security Glossary

AFI 65-201, *Management Control*

AFDIR 33-303, Compendium of Communications and Information Technology

AFSSI 4100VI, (FOUO) *The Air Force Communications Security (COMSEC) Program*

AFSSM 5019, *Computer Security Users Guide*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Vulnerability and Incident Reporting*

AFSSI 5024VI, *The Certification and Accreditation (C&A) Process*

AFSSI 5024VII, *The Certifying Official's Handbook*

AFSSI 5024VIII, *The Designated Approving Authority's Handbook* (when published)

AFSSI 5024VIV, *Type Accreditation* (when published)

AFSSI 5027, *Network Security Policy*

Abbreviations and Acronyms

ACC--Air Combat Command

ADP--Automated Data Processing

AFCA--Air Force Communications Agency

AFCERT--Air Force Computer Emergency Response Team

AFCIC--Air Force Communications and Information Center

AFI--Air Force Instruction

AFIWC--Air Force Information Warfare Center

AFMAN--Air Force Manual

AIA--Air Intelligence Agency

AFMC--Air Force Materiel Command

AFPD--Air Force Policy Directive

AFSSI--Air Force Systems Security Instruction

AFSSM--Air Force Systems Security Memorandum

ASIM--Automated Security Incident Monitoring

BIOS--Basic Input/Output System

C2--Class 2 (Controlled Access Protection)(a division and class of DoD 5200.28-STD

C&A--Certification and Accreditation

CCB--Configuration Control Board

CINC--Commander-in-Chief

CIO--Chief Information Officer

CJCSI--Chairman of the Joint Chiefs of Staff Instruction

COMPUSEC--Computer Security

COMSEC--Communications Security

CSM--Computer Systems Manager

CSO--Communications and Information Systems Officer

CSSO--Computer System Security Officer

DAA--Designated Approving Authority

DAC--Discretionary Access Control

DISA--Defense Information Systems Agency

DISN--Defense Information Systems Network

DoD--Department of Defense

DoDD--Department of Defense Directive

DRU--Direct Reporting Unit

DSAWG--DISN Security Accreditation Working Group

FOA--Field Operating Agency

FOUO--For Official Use Only

FTP--File Transfer Protocol

IA--Information Assurance

I&A--Identification and Authentication

IP--Information Protection

ITMRA--Information Technology Management Reform Act

JP--Joint Publication

MAC--Mandatory Access Control

MAJCOM--Major Command

NATO--North Atlantic Treaty Organization

NCC--Network Control Center

NCSC--National Computer Security Center

NIPRNET--Non-Secure Internet Protocol Router Network

OMB--Office of Management and Budget

PC--Personal Computer

P.L.--Public Law

POC--Point of Contact

SABI--Secret and Below Interoperability

SAF--Secretary of the Air Force

SATE--Security Awareness, Training, and Education

SIPRNET--Secret Internet Protocol Router Network

WM--Workgroup Manager

Y2K--Year 2000

Terms

Accountability--1. Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation. 2. (DoD) The obligation imposed by law or lawful order or regulation on an officer or other person for keeping accurate records of property, documents, or funds. The person having this obligation may or may not have actual possession of the property, documents, or funds. Accountability is concerned primarily with records while responsibility is concerned primarily with custody, care, and safekeeping. (JP 1-02)

Accreditation--1. Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls. 2. (DoD) In computer modeling and simulation, an official determination that a model or simulation is acceptable for a specific purpose. (JP 1-02)

Authenticity--Measure of the confidence that the security features and architecture of an information system accurately mediate and enforce the system security policy.

Category--A grouping of classified or sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval (e.g., formal access approval). Examples include proprietary, FOUO, Privacy Act, North Atlantic Treaty Organization (NATO), and compartmented information.

Certification--Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certifying Official--Individual responsible for making a technical judgment of the information systems compliance with stated security requirements and requesting approval to operate from the DAA.

Communications and Information Systems Officer (CSO)--At base level, the commander of the communications unit responsible for carrying out communications and information systems responsibilities. At MAJCOM, the person designated by the MAJCOM/CC responsible for overall management of communications and information systems budgeted and funded by that command. When no other office is formally designated as chief information officer (CIO), the CSO ensures compliance with the mandates of the Information Technology Management Reform Act (ITMRA) of 1996.

Computer-Based Security--Security for the information system is provided through the use of automated security features.

Computer Systems Manager (CSM)--Official with supervisory or management responsibility for an organization, activity, or functional area that owns or operates an information system. They are operationally and administratively responsible for the mission that the information system supports. They are responsible for the security-related functions within their office or facilities. (**NOTE:** This is not an appointed position. For office automation systems, the office chief or manager is normally the CSM.)

Computer Systems Security Officer (CSSO)--Official who manages the COMPUSEC program for an information system assigned to him or her by the CSM; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices.

Confidentiality--The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls--Prescribed actions taken to maintain the appropriate level of protection for information systems. Controls may validate security activities, detect security incidents and non-conformance, correct deficient security countermeasures, measure the assurance of information system activities, or report incidents. (**NOTE:** There are two divisions of control: management [policy, objectives, and criteria class] and internal [security requirements, mechanisms, and rules]. DoD 7740.1-G, *Department of Defense ADP Internal Control* Guideline, July 1998, outlines internal controls for information systems.)

Countermeasures--1. The sum of a safeguard and its associated controls. 2. (DoD) That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

Designated Approving Authority (DAA)--Official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Formal Access Approval--Documented approval by a data owner to allow access to a particular category of information.

Information--1. Data derived from observing phenomena and the instructions required to convert that data into meaningful information. (**NOTE:** Includes: operating system information such as system parameter settings, password files, audit data, etc.) 2. (DoD) Facts, data, or instructions in any medium or form. (JP 1-02) 3. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information System--1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (**NOTE:** This includes automated information systems.) 2. (DoD) The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

Integrity--Property that allows the preservation of known unaltered states between baseline certifications and allows information, access, and processing services to function according to specified expectations. It is composed of data and system integrity.

Level of Protection--Established safeguards with controls to counter threats and vulnerabilities based on the security requirements. Assures availability, integrity, and confidentiality of the information system.

Nonrepudiation--Method by which the sender of data is provided proof of delivery and the recipient is assured of the sender's identity so that neither can deny having processed the data.

Periods Processing--Processing of various levels of classified and unclassified information at distinctly different times. (**NOTE:** Under periods processing, the information system [operating in dedicated security mode] is purged of all information from one processing period before transitioning to the next when there are different users with different authorizations.)

Safeguards--Protective measures and controls prescribed to meet the security requirements of an information system. (**NOTE:** Safeguards include security features and management constraints from the various security disciplines [i.e., administrative, procedural, physical, personnel, communications, emanations, and computer security] used in concert to provide the requisite level of protection.)

Security Feature--A hardware-, firmware-, or software-controlled access protection to meet the security requirements of I&A; mandatory access control (MAC); discretionary access control (DAC); object reuse; or audit. Security features are a subset of information system security safeguards.

Sensitive Information--Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (**NOTE:** Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 [P.L. 100-235].)

Stand-Alone System--An information system physically and electronically isolated from all other systems and intended to be used by one user at a time, with no data belonging to other users remaining on the system (e.g., a PC with removable storage media such as a floppy disk).

Standard System--Two or more substantively similar information systems developed for the purpose of fielding multiple copies in support of a mission, within or across MAJCOM or service lines, or DoD-wide.

System Integrity--The attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Security Policy--Set of laws, rules, and practices that regulate how sensitive and classified information is managed, protected, and distributed by an information system. (**NOTE:** It interprets regulatory [e.g., DoDD 5200.28, AFPD 33-2, AFI 33-202, etc.] and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks, regardless of their sensitivity, criticality, or life-cycle phase, will have a system security policy.)

Tampering--Unauthorized modification that alters the proper functioning of information system security equipment.

Threat--Current and perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, fraud, waste, or abuse to a system.

User--Person or process accessing an information system by direct connections (e.g., via terminals) or indirect connections.

Vulnerability--1. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. 2. (DoD) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 1-02) 3. (DoD) The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1-02)

Workgroup Manager (WM)--A duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems.